UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,500	10/12/2001	Peter Yeung	031941-094	3432

27045 7590 01/06/2005

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR C11
PLANO, TX 75024

EXAMINER	
AHMED, FAROOQUE	
ART UNIT	**PAPER NUMBER**
2157	

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/976,500	YEUNG ET AL.	
	Examiner	Art Unit	
	Farooque Ahmed	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/12/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the application filed 10/12/2001. Claims 1-34 are pending. Claims 1-21 represent System and a method relating to access control

Claim Objections

2. Claims 12-14 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim. See MPEP § 608.01(n). Accordingly, the claims12-14 are not been further treated on the merits.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1,24,29,30,32,are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out" comprising or communicating" "characterized ""data/fetching" and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1,3,6,12,16,24,29,30, the phrase "for example" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

4. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. Claims 1-34 are rejected under 35 USC § 102(e) as being anticipated by Jerger ret al., U.S. patent no. 6,321,334.

Jerger teaches the invention as claimed include a computer system method and network with security policy configured by user. (see abstract)

As claim 1, Jerger system for end user control of the distribution and maintenance of end user personal profile data in a data communications system providing communication between applications comprising and/or communicating with service/information/content providers or holding means (DB) holding end user personal profile data, characterized in

that it comprises a personal profile protection network with at least one central protection server means (see col. 3 lines 5-67col 4 lines 14-65 Jerger disclose web server with firewall protection and Active X);

comprising or communicating with information holding means holding personal protection profile information, and a number of distributed access means, e.g. software modules, whereby for each of said applications at least one access (See col. 3 lines 5-67col 4 lines 14-65, Jerger disclose web server with user data directory access with multiple application);

means is provided, and in that grant/reject of an access request for/to end

user personal profile data by a requesting application is determined by the central protection server in communication with a requesting application and/or an information providing applications in that translating means are provided for identity translation and that the identity of a requesting application will be concealed for an information providing application, and vice versa (See col. 3 lines 5-67col 4 lines 14-65, Jerger disclosed User access its documents through web application. User enables a protection during the communication with web server).

As to claim 2, Jerger teaches the system as recited in claim 1, characterized in that there is one access means for each application (See col.1 lines 12-67, Jerger disclose that the client use the web application to access data).

As to claim 3, Jerger teaches the system as recited in claim 1, characterized in that there are a plurality, e.g. a cluster, of access means for at least one application (see figs 1-13 col.1 lines 12-67; col 10, lines 18-45, Jerger disclosed plurality server where client use web application to access the data).

As to claim 4, Jerger teaches the system as recited in claim 1, 2 or 3, characterized in that the central server means only comprises personal protection profile data, the personal profile data being distributed throughout the system (see col10. lines18-67, Jerger disclose that user data is stored in the server directory).

As to claim 5, Jerger teaches the system as recited in claim 4, characterized in that the personal protection profile data comprises information about, for each end user of the system, which of the end user personal profile data that should be accessible by which application (see col10. lines18-67, Jerger disclose that user various data information can be access from multiple application which is stored in web server directory).

As to claim 6, Jerger teaches the system as recited in claim 4, characterized in that the personal protection profiles are assigned one of a given number of security levels, the lowest level e.g. indicating that for all personal profile data access is prevented for every application, the highest e.g. indicating that all personal profile data is freely available (col. 14, lines 4-64, Jerger disclose that User enable the security to data profile in web server).

As to claim 7, Jerger teaches the system as recited in any one of the preceding claims, characterized in that the interface between an application and the respective access means comprises an Application Programmable Interface (API) based on (using) a generic markup language (See fig 4A-9g col13, lines 48-67; col. 14, lines 4-64, Jerger disclosed The application interface based on HTML).

As to claim 8, Jerger teaches the system as recited in claim 7, characterized in that the generic markup language is XML (col. 14, lines 4-64, Jerger disclose Application interface based on HTML, JavaM).

As to claim 9, Jerger teaches the system as recited in claim 7 or 8, characterized in that access to requested end user personal profile data is granted/rejected by the central server in communication with the requesting application (see Fig 2-9 col. 15 lines 5-67; col 16, Jerger disclose The web application where access are granted to user based on security).

As to claim 10, Jerger teaches the system as recited in claim 7 or 8, characterized in that access to requested end user personal profile data is granted/rejected by the central server in communication with the information providing application (See fig 3-13 col.3; col 4 Jerger disclose that user access the data directory in web server based on permission).

As to claim 11, Jerger teaches the system as recited in claim 7 or 8, characterized in that access to requested end user personal profile data is granted/rejected by the central server in communication with the requesting application and the information providing application (See fig 3-13 col.3; col 4 Jerger disclose that user access the data directory in web application based on permission).

As to claim 12, Jerger teaches the system as recited in claim 9, 10 or 11, characterized in that first user identity translating means (e.g. encrypting means) are provided at least in the central server means (See fig 3-19 col.31; col 40, Jerger disclose user access the data directory in web server based on log on permission).

As to claim 13, Jerger teaches the system as recited in claim 9, 11 or 12, characterized in that second user identity translating means are provided in the access

means of the requesting application. See fig 3-19 col.31; col 40, Jerger disclose that user access the data directory in web server based on log on permission).

As to claim 14, Jerger teaches the system as recited in claims 17-13, characterized in that for each pair of applications of the system a general DTD (Document Type Definition) is given to define allowed flow of personal data (See col 3 lines 27-65, Jerger disclose Document type data is session between client and server).

As to claim 15, Jerger teaches the system as recited in claim 14, characterized in that for each user a specific user unique DTD agreement is given (See col. 3 lines 27-65, Jerger disclosed Document type data is session between client and server).

As to claim 16, Jerger teaches the system as recited in claim 17-15, characterized in that an access request for end user profile data is transported from the requesting application to its access means e.g. using RMI, and in that the access request includes a user identity associated with the requested personal end user Profile (See col.3 lines 27 –67, Jerger disclosed user data where security is applied on the application).

As to claim 17, Jerger teaches the system as recited in claim 116, characterized in that the request is transported as an XML transport object (XML Node tree container) tagged with information about the requested end user personal profile data (see figs 4A-9G, col 21 lines 28 –67 Jerger disclose the tree view displaying user information).

As to claim 18, Jerger teaches the system as recited in claim16 or 17, characterized in that the HTTPS protocol is used for communication between the access means of the requesting/information holding application and the central server means (see col.1lines 25- 67, Jerger disclosed HTTP protocol to access web server).

As to claim 19, Jerger teaches the system as recited in any one of the preceding claims, characterized in that the access means of the information requesting and/or providing application(s) comprise(s) means for encrypting the user identity associated with the requested end user profile (See figs 3-19, col.37, Jerger disclose user access a the web server where identification is encryption to match the directory).

As to claim 20, Jerger teaches the system as recited in any one of the preceding claims, characterized in that the request is digitally signed with a private key of the access means of the requesting application and/or with a private key of the access means of the information providing application (See figs 10-19,col. 29 lines 47-67; col. 31 lines 17, Jerger disclose private/public key is part of digital signature to access to web application).

As to claim 21, Jerger teaches the system as recited in claim 120, characterized in that the request is digitally signed with a private key of the central server means, and in that the digital signature(s) of the access means are verified in the central server (See figs 10-19,col. 29 lines 47-67; col. 31 lines 17 –65, Jerger disclose private key is part of digital signature to access to network).

As to claim 22, Jerger teaches the system as recited in claim 21, characterized in that the central server means comprises means for encrypting at least the user identity associated with the requested information used by the information providing information (See figs 3-19 col.37, Jerger disclose that user access a the web server based on identification is encryption to directory).

As to claim 23, Jerger teaches the system as recited any one of the preceding claims, characterized in that at least some of the applications comprise a cache memory respectively for temporarily holding information about access requests, such that a previously used session can be reused, at least for a given time period (see figs 3-13, col 14 lines 45-67 Jerger disclose web server holding a user information in memory based on session).

As claim 24, Jerger teaches personal profile (privacy) control network for controlling the access to personal profile data, characterized in that it comprises

at least one central protection server means, comprising or communicating with information holding (see col. 3 lines 5-67col 4 lines 14-65 Jerger disclose web server with firewall protection);

means holding personal protection profile information, and a number of distributed access means, e.g. software modules, at least one access means respectively interfacing each of a number of applications, the central

protection server means comprising (See col. 3 lines 5-67col 4 lines 14-65, Jerger disclose the web server with user data directory access with multiple application);

means for translating and verifying identities, and in that a request for access to personal profile data by a requesting application is communicated to the requesting application access means and granted/rejected by the central server means in communication with the access means of the requesting application and/or the information providing application, and in that the user identity used by the requesting application is concealed for the information providing application and vice versa (See col. 3 lines 5-67col 4 lines 14-65, Jerger disclose User access its documents through web application. User enable a protection during the communication with web server).

As to claim 25, Jerger teaches personal profile control network according to claim 24, characterized in that the interface between an application and the respective access means is based on a generic mark-up language (See Fig 4A-9G Col. 14, lines 4-64, Jerger disclosed Application interface based on HTML).

As to claim 26, Jerger teaches personal profile control network according to claim 25, characterized in that the generic mark-up language is XML (See Fig 4A-9G, col. 14, lines 4-64, Jerger disclose the Application interface based on HTML, JavaM Code).

As to claim 25, Jerger teaches personal profile control network according to claim any one of claims 24-26, characterized in that the information holding means of the central server means comprises, for each user of the system, a personal protection profile, and in that the personal protection profiles are end user controlled (see Fig 4A-9G, col.21 Lines 9-67, Jerger disclose the web serve with user directory are maintained by user).

As to claim 25, Jerger teaches personal profile control network according to claim 27, characterized in that the central server means and at least one of the information requesting/providing access means digitally sign a request for personal profile data with the respective private key, and in that the digital signatures are

verified by the central server means (See figs 10-13, col. 29 lines 47-67; col. 31 lines 17 -Jerger disclose private/public key is part of digital signature to access web server).

As to claim 29 Jerger teaches method of controlling access to personal data within a personal end user profile in a data communication network running a number of applications comprising or communicating with information holding means, characterized in that it comprises the steps of:

providing an access request from a requesting application to an access means associated with the requesting application using a generic mark-up language, e.g. XML, forwarding the request from the access (see figs 1-19 col. 14, lines 4-64, Jerger disclose access the web server from Application interface based on HTML, JavaM).

means to a central server means with information holding means holding personal protection profiles for the end users in the system; performing user identification encryption, such that the user identification of the requesting application will be concealed from an information providing application, and vice versa; establishing, by using the request and the personal protection profile whether access is to be granted or denied; (See figs 1-19 col. 3 lines 5-67col 4 lines 14-65, Jerger disclosed User access its documents through web application. User enables a protection during the communication with web server).

if access to the requested personal profile is to be granted, confirming to the access means of the requesting application whether access is to be granted or not, preferably after digitally signing the request; allowing transfer of the encrypted and preferably digitally signed request to the information providing application. See figs 1-19,col. 29 lines 47-67; col. 31 lines 17 –65, Jerger disclose access the web server where private key is part of digital signature to access to network);

As to claim 30, Jerger teaches method according to claim 29, characterized in that the request of a requesting application relates to getting access to data/fetching data in a personal profile and in that, for a granted request, the method comprises the

step of:

transferring the requested data via the access means of an information providing application over a data communication network, e.g. Internet, to the access means of the requesting application (see fig1-9, col. 3 lines 27- 65, Jerger disclose the client and web server exchange information over web application).

As to claim 31, Jerger teaches method according to claim 29, characterized in that the request of a requesting application relates to setting/updating data in a personal profile, and in that, for a granted request the method further comprises the step of:

transferring the data to be set/updated data to the information providing application over the data communication network (see fig 1-3 col. Lines 10-67, Jerger disclosed transferring data from web server to client pc).

As claim method of controlling access to personal data within a personal end user profile in a data communication network running a number of applications comprising, or communicating, with information holding means, characterized in that it comprises the steps of:

forwarding a request for access to data within a personal profile from a requesting application via at least one distributed access means to a central server means (see figs 1-13 col. 4 lines Jerger disclose web server with client directory with multiple application access).

establishing in the central server means whether access to requested data should be allowed or not by comparing the request with an end user controlled personal protection profile (See col. 3 lines 5-67col 4 lines 14-65, Jerger disclose web server with user data directory access with multiple application);

providing the at least one distributed access means with information as to whether access is allowable or not, such that if access is allowable, the data communication network can be used for giving the requesting application access to the requested data without the identity of the requesting application being visible to the application able to provide access to the requested data, and vice

versa. (See col. 3 lines 5-67col 4 lines 14-65, Jerger disclose User access its documents through web application. User enable a protection during the communication with web server).

As to claim 33, Jerger teaches method according to claim 32, characterized in that it further comprises the steps of: encrypting a user identity associated with the requested end user profile into the request at the central server means or at access means associated with the requesting application;

decrypting the user identity at access means associated with the information providing application (See figs 1-19 col. 31 lines 13-64, Jerger disclose decryption the publisher key in internet security manger).

As to claim 34, Jerger teaches method according to claim 32 or 33, characterized in that it comprises the steps of: digitally signing the request at one or more of the access means associated with the information requesting application, the access means associated with the information providing application and the central server means, said access means and the central server means constituting a personal profile data protection network (See fig 1-9 col. 4 lines 28-67, Jerger teaches user access the file on web server through application).

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farooque Ahmed whose telephone number is 703-605-4212. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (703)308-7562. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farooq Ahmed
ART UNIT 2157

SALEH NAJJAR
PRIMARY EXAMINER